CLAIMS

What is claimed is:

1. A method of creating a certificate revocation list (CRL), comprising:

a) creating a single CRL that is centralized, said single CRL associated with a certificate authority (CA) comprising a master server coupled to a plurality of CA clone servers;

b) maintaining said single CRL with said master server;

c) receiving notice, from one of said plurality of CA clone servers, at said master server containing revocation information regarding a certificate; and

d) updating said single CRL according to said revocation information.

2. The method of creating a CRL as described in Claim 1, wherein step d) comprises:

adding said certificate to said single CRL when said revocation information indicates said certificate is revoked, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.

3. The method of creating a CRL as described in Claim 1, wherein step d) comprises:

removing said certificate from said single CRL when said revocation information indicates said certificate is valid, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.

4. The method of creating a CRL as described in Claim 1, further comprising:

maintaining said single CRL with a CRL merger service module located at said master server.

5. The method of creating a CRL as described in Claim 1, further comprising:

sending said notice over a secure communications channel.

6. The method of creating a CRL as described in Claim 5, further comprising:

at said one of said cluster of servers, performing secure sockets layer (SSL) client authentication over said secure communications channel before sending said notice over said secure communications channel.

7. The method of creating a CRL as described in Claim 1, further comprising:

transmitting said single CRL that is updated to a recipient over a communication network.

8. The method of creating a CRL as described in Claim 1, further comprising:

providing certificate authority services not including maintaining and managing said single CRL at each of said plurality of CA clone servers.

9. The method of creating a CRL as described in Claim 1, further comprising:

storing said CRL in a database accessed via a lightweight directory access protocol (LDAP) that supports a Secure Sockets Layer (SSL).

10. The method of creating a CRL as described in Claim 1, further comprising:

at said one of said plurality of clone servers, detecting whether said notice was received at said master server;

repeatedly sending said notice until received by said master server.

11. The method of creating a CRL as described in claim 10, further comprising:

storing said notice if said notice was not received at said master server.

12. In a certificate authority (CA) having a plurality of clone servers, a method generating and maintaining certificate revocation list information, comprising:

a) each of said clone servers independently generating revocation information relating to certificates;

b) sending said revocation information to a master server coupled to said plurality of clone servers; and

c) maintaining a single centralized certificate revocation list (CRL) based on said revocation information from said plurality of clone servers, said step c) performed by said master server.

13. The method as described in Claim 12, further comprising:

d) in response to an inquiry for said CRL, providing said CRL on behalf of said CA, said step d) performed by said master server.

14. The method as described in Claim 12, further comprising:

d) based on said revocation information, adding a certificate to said CRL when said revocation information indicates said certificate is revoked.

15. The method as described in Claim 12, further comprising:

d) based on said revocation information, removing a certificate from said CRL when said revocation information indicates said certificate is valid.

16. A certificate authority (CA) comprising:

a plurality of clone servers coupled together for providing certificate authority services;

a centralized certificate revocation list (CRL) associated with said CA; and

a master server coupled to said plurality of clone servers for maintaining said centralized CRL based on revocation information from said plurality of clone servers.

17. The CA as described in Claim 16, wherein said master server adds a certificate to said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate has been revoked.

18. The CA as described in Claim 16, wherein said master server removes a certificate from said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate is valid.

19. The CA as described in Claim 16, further comprising:

a secure communication network coupling each of said plurality of clone servers to said master server for providing secure communication when said information is sent between said plurality of clone servers and said master server.

20. The CA as described in Claim 16, further comprising:

a lightweight directory access protocol (LDAP) database that is coupled to said master server for storing said centralized CRL.

21. The CA as described in Claim 16, further comprising:

a CRL merger service module located at said master server for maintaining said CRL.

22. A certificate authority (CA) comprising:

a plurality of clone servers coupled together for providing certificate authority services;

a centralized certificate revocation list (CRL) associated with said CA, said centralized CRL located in a lightweight directory access protocol (LDAP) database; and

a master server coupled to said plurality of clone servers for maintaining said centralized CRL based on revocation information from said plurality of clone servers, said centralized CRL coupled to said merger server.

23. The CA as described in Claim 22, wherein said master server adds a certificate to said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate has been revoked.

24. The CA as described in Claim 22, wherein said master server removes a certificate from said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate is valid.